AMENDMENTS TO THE CLAIMS

1-84. (Canceled)

85. (Currently Amended) A method for controlling a terminal apparatus, the terminal apparatus being connected to a network, the network including i) a content distribution server, ii) a metadata distribution server, iii) a license management server and iv) an authentication server, i) the content distribution server storing content and a content provider ID, and generating (a) a public key certificate of the metadata distribution server that is authorized by the content distribution server which includes a subject ID indicating the metadata distribution server, and (b) a digital sign for the subject ID, the public key certificate also including a certificate signer ID identifying a signer that digitally signs the public key certificate, ~~the content provider ID being information for identifying a content provider providing the content,~~ ii) the metadata distribution server storing metadata, the metadata being used for supplementing the content, the metadata including a metadata signer ID, the metadata signer ID indicating a signer that digitally signs the metadata, iii) the license management server storing usage control information for the content and the metadata, the usage control information including signer identification information, the signer identification information identifying a range of a provider that is permitted to provide the metadata to the terminal apparatus, iv) the authentication server receiving from one of the content distribution server and the metadata distribution server a request for a generation of a public key certificate, generating a subject ID indicating the one of the content distribution server and the metadata distribution server that transmits the request to the authentication server, generating a digital sign for the subject ID, and generating the public key certificate including the subject ID and the digital sign, the public key certificate also

including a certificate signer ID, the certificate signer ID identifying a signer that digitally signs the public key certificate, the method comprising:

receiving, at the terminal apparatus, the content and the content provider ID stored in the content distribution server;

receiving, at the terminal apparatus from the license management server, the usage control information;

receiving, at the terminal apparatus from the metadata distribution server, the metadata;

receiving, at the terminal apparatus, the public key certificate generated by the authentication server or the content distribution server;

judging, at the terminal apparatus, whether the received content provider ID matches the metadata signer ID included in the metadata, when the range included in the usage control information indicates i) the content distribution server or ii) the content distribution server and the metadata distribution server that is authorized by the content distribution server;

judging, at the terminal apparatus, whether the received content provider ID matches the certificate signer ID included in the public key certificate whose subject ID matches the metadata signer ID, when it is judged that the content provider ID does not match the metadata signer ID and when the range included in the usage control information indicates the content distribution server and the metadata distribution server that is authorized by the content distribution server; and

determining, at the terminal apparatus, that the metadata is available to the terminal apparatus, i) when it is judged that the content provider ID matches the metadata signer ID or ii) when it is judged that the content provider ID matches the certificate signer ID.

86. (Previously Presented) The method according to Claim 85,

wherein the metadata comprises user metadata generated by a user of the terminal apparatus.

87. (Previously Presented) The method according to Claim 86,

wherein the user metadata does not include the metadata signer ID.

88. (Previously Presented) The method according to Claim 86,

wherein the user metadata is encrypted by secret information common to one or more terminal apparatuses owned by the user of the terminal apparatus.

89. (Previously Presented) The method according to Claim 85,

wherein the usage control information includes revision permission information, the revision permission information indicating whether the metadata is permitted to be revised, and

the method further comprises judging whether the metadata is permitted to be revised based on the revision permission information, when it is determined that the metadata is available to the terminal apparatus.

90. (Previously Presented) The method according to Claim 86,

wherein the usage control information includes control permission information, the control permission information indicating whether the user metadata is permitted to be used, and

the method further comprises judging whether the user metadata is permitted to be used based on the control permission information.

91. (Previously Presented) The method according to Claim 86,

wherein the user metadata is encrypted by a predetermined encryption key,

wherein the usage control information includes control permission information, the control permission information indicating whether the user metadata is permitted to be used,

wherein the usage control information includes moving range specifying information, the moving range specifying information indicating whether the user metadata is permitted to be moved out of the terminal apparatus, and

wherein the method further comprises:

judging whether the user metadata is permitted to be used based on the control permission information;

judging whether the user metadata is permitted to be moved out of the terminal apparatus based on the moving range specifying information, when it is judged that the user metadata is permitted to be used based on the control permission information; and

decrypting the user metadata using a predetermined decryption key corresponding to the predetermined encryption key.

92. (Previously Presented) The method according to Claim 91,

wherein the predetermined encryption key comprises secret information common to one or more terminal apparatuses owned by the user of the terminal apparatus.

93. (Currently Amended) A terminal apparatus being connected to a network, the network including a content distribution server, a metadata distribution server, a license management server and an authentication server, the content distribution server storing content

and a content provided ID, and generating (a) a public key certificate of the metadata distribution server that is authorized by the content distribution server which includes a subject ID indicating the metadata distribution server, and (b) a digital sign for the subject ID, the public key certificate also including a certificate signer ID identifying a signer that digitally signs the public key certificate, the terminal apparatus comprising:

a storage unit;

a receiving unit for i) receiving the content and the [[a]] content provider ID stored in the content distribution server, ~~the content provider ID being information for identifying a content provider providing the content,~~ ii) receiving metadata stored in the metadata distribution server, the metadata being used for supplementing the content and including a metadata signer ID, the metadata signer ID indicating a signer that digitally signs the metadata, iii) receiving, from the license management server, usage control information for the content and the metadata, the license management server storing the usage control information for the content and the metadata, the usage control information including signer identification information, the signer identification information identifying a range of a provider that is permitted to provide the metadata to the terminal apparatus, and iv) receiving a public key certificate generated by the authentication server or the content distribution server, the authentication server receiving from one of the content distribution server and the metadata distribution server a request for a generation of the public key certificate, generating a subject ID indicating the one of the content distribution server and the metadata distribution server that transmits the request to the authentication server, generating a digital sign for the subject ID, and generating the public key certificate including the subject ID and the digital sign, the public key certificate also including a

certificate signer ID, the certificate signer ID identifying a signer that digitally signs the public key certificate; and

a judging unit for i) judging whether the received content provider ID matches the metadata signer ID included in the metadata, when the range included in the usage control information indicates a) the content distribution server or b) the content distribution server and the metadata distribution server that is authorized by the content distribution server, ii) judging whether the received content provider ID matches the certificate signer ID included in the public key certificate whose subject ID matches the metadata signer ID, when it is judged that the content provider ID does not match the metadata signer ID and when the range included in the usage control information indicates the content distribution server and the metadata distribution server that is authorized by the content distribution server, and iii) determining that the metadata is available to the terminal apparatus, a) when it is judged that the content provider ID matches the metadata signer ID or b) when it is judged that the content provider ID matches the certificate signer ID.

94. (Currently Amended) A system comprising:

a content distribution server for storing content and a content provider ID, ~~the content provider ID being information for identifying a content provider providing the content~~ and generating (a) a public key certificate of the metadata distribution server that is authorized by the content distribution server which includes a subject ID indicating the metadata distribution server, and (b) a digital sign for the subject ID, the public key certificate also including a certificate signer ID identifying a signer that digitally signs the public key certificate;

a metadata distribution server storing metadata, the metadata being used for supplementing the content, the metadata including a metadata signer ID, the metadata signer ID indicating a signer that digitally signs the metadata;

a license management server for storing usage control information for the content and the metadata, the usage control information including signer identification information, the signer identification information identifying a range of a provider that is permitted to provide the metadata to the terminal apparatus;

an authentication server for receiving from one of the content distribution server and the metadata distribution server a request for a generation of a public key certificate, generating a subject ID indicating the one of the content distribution server and the metadata distribution server that transmits the request to the authentication server, generating a digital sign for the subject ID, and generating the public key certificate including the subject ID and the digital sign, the public key certificate also including a certificate signer ID, the certificate signer ID identifying a signer that digitally signs the public key certificate; and

a terminal apparatus, the terminal apparatus comprising:

a receiving unit for receiving the content and the content provider ID stored in the content distribution server, receiving from the license management server the usage control information, receiving from the metadata distribution server the metadata, and receiving the public key certificate generated by the authentication server or the content distribution server; and

a judging unit for judging whether the received content provider ID matches the metadata signer ID included in the metadata, when the range included in the usage control information indicates i) the content distribution server or ii) the content

distribution server and the metadata distribution server that is authorized by the content distribution server, judging whether the received content provider ID matches the certificate signer ID included in the public key certificate whose subject ID matches the metadata signer ID, when it is judged that the content provider ID does not match the metadata signer ID and when the range included in the usage control information indicates the content distribution server and the metadata distribution server that is authorized by the content distribution server, and determining that the metadata is available to the terminal apparatus, i) when it is judged that the content provider ID matches the metadata signer ID or ii) when it is judged that the content provider ID matches the certificate signer ID.

95. (Currently Amended) A computer-readable recording medium storing a program, the program controlling a terminal apparatus, the terminal apparatus being connected to a network, the network including i) a content distribution server, ii) a metadata distribution server, iii) a license management server and iv) an authentication server, i) the content distribution server storing content and a content provider ID, and generating (a) a public key certificate of the metadata distribution server that is authorized by the content distribution server which includes a subject ID indicating the metadata distribution server, and (b) a digital sign for the subject ID, the public key certificate also including a certificate signer ID identifying a signer that digitally signs the public key certificate, ~~the content provider ID being information for identifying a content provider providing the content,~~ ii) the metadata distribution server storing metadata, the metadata being used for supplementing the content, the metadata including a metadata signer ID, the metadata signer ID indicating a signer that digitally signs the metadata, iii) the license

management server storing usage control information for the content and the metadata, the usage control information including signer identification information, the signer identification information identifying a range of a provider that is permitted to provide the metadata to the terminal apparatus, iv) the authentication server receiving from one of the content distribution server and the metadata distribution server a request for a generation of a public key certificate, generating a subject ID indicating the one of the content distribution server and the metadata distribution server that transmits the request to the authentication server, generating a digital sign for the subject ID, and generating the public key certificate including the subject ID and the digital sign, the public key certificate also including a certificate signer ID, the certificate signer ID identifying a signer that digitally signs the public key certificate, the computer program controlling the terminal apparatus to execute a following method, the method comprising:

receiving, at the terminal apparatus, the content and the content provider ID stored in the content distribution server;

receiving, at the terminal apparatus from the license management server, the usage control information;

receiving, at the terminal apparatus from the metadata distribution server, the metadata;

receiving, at the terminal apparatus, the public key certificate generated by the authentication server or the content distribution server;

judging, at the terminal apparatus, whether the received content provider ID matches the metadata signer ID included in the metadata, when the range included in the usage control information indicates i) the content distribution server or ii) the content distribution server and the metadata distribution server that is authorized by the content distribution server;

judging, at the terminal apparatus, whether the received content provider ID matches the certificate signer ID included in the public key certificate whose subject ID matches the metadata signer ID, when it is judged that the content provider ID does not match the metadata signer ID and when the range included in the usage control information indicates the content distribution server and the metadata distribution server that is authorized by the content distribution server; and

determining, at the terminal apparatus, that the metadata is available to the terminal apparatus, i) when it is judged that the content provider ID matches the metadata signer ID or ii) when it is judged that the content provider ID matches the certificate signer ID.